IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF DELAWARE

BEN REDMOND; LINDSAY RATHERT; SALVADOR RAMIREZ; GERRY GALIPAULT; KYLE WESTENDORF, ROBERT WOODS, and JORDAN HUNSTONE, individually and on behalf of all others similarly situated, Plaintiffs, v. FACEBOOK, INC.; GLOBAL SCIENCE RESEARCH LTD; ALEKSANDR KOGAN; SCL GROUP LIMITED; SCL ELECTIONS LTD; SCL USA INC.; CAMBRIDGE ANALYTICA LLC; CAMBRIDGE ANALYTICA HOLDINGS LLC; CAMBRIDGE ANALYTICA COMMERCIAL LLC; and CAMBRIDGE ANALYTICA POLITICAL LLC, Defendants.	Case No. **CLASS ACTION COMPLAINT FOR:** 1. Violation of Stored Communication Act, 18 U.S.C. § 2071, *et seq.* 2. Fraud 3. Negligence 4. Willful Negligence

CLASS ACTION COMPLAINT

Plaintiffs, Ben Redmond, Lindsay Rathert, Salvador Ramirez, Gerry Galipault, Kyle Westendorf, Robert Woods, and Jordan Hunstone on behalf of themselves and all others similarly situated, by and through their undersigned counsel, upon knowledge as to themselves and otherwise upon information and belief, allege against Defendants Facebook, Inc. ("Facebook"); Global Science Research Ltd. ("GSR"); Aleksandr Kogan ("Kogan"); SCL Group Limited; ("SCL Group"); SCL Elections Ltd. ("SCL Elections"); SCL USA Inc. ("SCL USA") (collectively "SCL Entities"); Cambridge Analytica LLC; Cambridge Analytica Holdings LLC; Cambridge Analytica

Commercial LLC; and Cambridge Analytica Political LLC (collectively "Cambridge," and together with Facebook and SCL Entities, "Defendants") as follows:

SUMMARY OF CLAIMS

1. This is a class action lawsuit brought by Plaintiffs on behalf of similarly situated individuals who are registered users of Facebook and whose personal information was improperly and without authorization accessed and/or obtained by GSR, Kogan, SCL Entities and Cambridge.

2. In 2011, Facebook entered into a consent decree with the Federal Trade Commission that required Facebook to, *inter alia*, "not misrepresent in any manner, expressly or by implication, the extent to which it maintains the privacy or security of covered information, including, but not limited to: … (C) the extent to which [Facebook] makes or has made covered information accessible to third parties;"[1]

3. Covered information is defined in the FTC Consent Order as:

> [I]nformation from or about an individual consumer including, but not limited to: (a) a first or last name; (b) a home or other physical address, including street name and name of city or town; (c) an email address or other online contact information, such as an instant messaging user identifier or a screen name; (d) a mobile or other telephone number; (e) photos and videos; (f) Internet Protocol ("IP") address, User ID or other persistent identified; (g) physical location; or (h) any information combined with any of (a) through (g) above.[2]

4. Further, Facebook was ordered to:

> [I]n connection with any product or service, in or affecting commerce, prior to any sharing of a user's nonpublic information by [Facebook] with any third party, which materially exceeds the restrictions imposed by a user's privacy setting(s), shall: A. clearly and prominently disclose to the user, separate and apart from any "privacy policy," "data use policy," "statement of rights and responsibilities" page, or other similar document: (1) the categories of nonpublic user information that will be disclosed to such third parties, (2) the identity or specific categories of such third parties, and (3)

[1] *In the Matter of Facebook, Inc., a corporation*, Agreement Containing Consent Order, at Section I.C. ("FTC Consent Order").
[2] FTC Consent Order, at Section Definitions, 4.

> that such sharing exceeds the restrictions imposed by the privacy setting(s) in effect for the user; and B. obtain the user's affirmative express consent.[3]

5. In 2014, Defendants GSR, Kogan, SCL Entities, and Cambridge improperly, and without authorization, in violation of the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.*, obtained the personal information of approximately 87 million registered Facebook users, approximately 70.6 million of whom were in the U.S. and approximately 1 million of which were in the U.K.,[4] without their knowledge, consent, or authorization.[5] This information included the users' full names, telephone numbers, mailing addresses, email addresses, ages, interests, physical locations, political and religious affiliations, relationships, pages they have liked, and groups to which they belong.

6. Defendant Facebook, contrary to the representations, obligations, and promises made to the federal government in 2011, knowingly set up its platform such that a third-party application developer who gained access to a user through an application could also access the personal information and data of that user's friends in violation of the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.* In addition, Facebook negligently failed to protect its users' data from such unauthorized access by a third party; upon learning about this unauthorized access and use of the personal data, failed to take reasonable steps required to claw back or, in the alternative, ensure the destruction of this data; and failed to notify its users' that such a breach had occurred, only admitting to the breach after their negligence was disclosed by a whistleblower.

[3] FTC Consent Order, at Section II.A. and II.B.

[4] https://www.wsj.com/articles/mark-zuckerberg-to-testify-before-house-committee-on-april-11-1522844990?emailToken=b6039753815a6fb549210722e887f14av3KEs4TOaQIbKRrbYLLs22td%2FrKp5yfbe9pQQP3CdaSDUFWHvMhLvQCKo0tPnnazCRiOHRE%2BOT4%2FvgEOjHfZM38dqDgrgkiLq4nc328MDuGOUQ2xG%2FtuMgpFdsknnvTH

[5] Because the proposed Class includes only those users from the United States and the U.K., we will use the 71.6 million number throughout the Complaint.

JURISDICTION AND VENUE

7. This Court has personal jurisdiction over Defendants Facebook, SCL USA Inc., Cambridge Analytica LLC, Cambridge Analytica Holdings, LLC, Cambridge Analytica Commercial LLP, and Cambridge Analytica Political LLC because they are each incorporated under the laws of Delaware.

8. This Court has personal jurisdiction over Defendants GSR, Kogan, SCL Group Limited, and SCL Elections Ltd because; (i) Defendant SCL USA Inc. is the alter ego of SCL Group Limited and SCL Elections Ltd; (ii) GSR is the alter ego of Kogan; (iii) they each entered into a contract which required, by its very terms, an impact on U.S. citizens, including those located in Delaware;[6] (iv) they have each done business in Delaware and have caused tortious injury in Delaware; and (v) because, on information and belief, Defendants GSR, Kogan, SCL Group Limited and SCL Elections Ltd took steps to improperly evade jurisdiction in this district by utilizing non-U.S. employees for work undertaken in the U.S.[7]

9. This Court has subject matter jurisdiction over this action and each Defendant pursuant to 28 U.S.C. § 1331 because this action arises under federal statute, namely the Stored Communication Act, 18 U.S.C. § 2701, *et seq.* ("SCA") and pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d) ("CAFA") because the aggregate amount in controversy exceeds $5,000,000, exclusive of interests and costs, there are more than 100 class members, and at least one class member is a citizen of a state different from Defendants and is a citizen of a foreign state.

[6] *See*, Contract between Global Services Research Ltd and SCL Elections Ltd, attached hereto as Exhibit 1 ("GSR Contract"), at Schedule 1.

[7] https://www.thestar.com/news/world/2018/03/25/former-cambridge-analytica-workers-say-firm-sent-foreigners-to-advise-us-campaigns html; https://www.theguardian.com/uk-news/2018/mar/17/cambridge-analytica-non-american-employees-political

10. Venue is proper in this District because each of the Defendants either conducts business in this District and/or is incorporated under the laws of Delaware.

THE PARTIES

11. Plaintiff Ben Redmond is an adult domiciled in California. Mr. Redmond has been registered with Facebook since at least 2007 and did not utilize or otherwise access the application *thisisyourdigitallife.com*.

12. Plaintiff Lindsay Rathert is an adult domiciled in Illinois. Ms. Rathert has been registered with Facebook at least since 2004 and did not utilize or otherwise access the application *thisisyourdigitallife.com*.

13. Plaintiff Kyle Westendorf is an adult domiciled in Ohio. Mr. Westendorf has been registered with Facebook at least since 2006 and did not utilize or otherwise access the application *thisisyourdigitallife.com*.

14. Plaintiff Salvador Ramirez is an adult domiciled in Texas. Mr. Ramirez has been registered with Facebook at least since 2005 and did not utilize or otherwise access the application *thisisyourdigitallife.com*.

15. Plaintiff Gerry Galipault is an adult domiciled in Florida. Mr. Galipault has been registered with Facebook at least since 2008 and did not utilize or otherwise access the application *thisisyourdigitallife.com.*

16. Plaintiff Robert Woods is an adult domiciled in Greater London, England. Mr. Woods has been registered with Facebook at least since 2007 and did not utilize or otherwise access the application *thisisyourdigitallife.com*.

17. Plaintiff Jordan Hunstone is an adult domiciled in Great Manchester, England. Mr. Hunstone has been registered with Facebook at least since 2012 and did not utilize or otherwise access the application *thisisyourdigitallife.com.*

18. Defendant Facebook, Inc. ("Facebook") is incorporated in Delaware and has its principal executive offices at 1 Hacker Way, Menlo Park, California 94025 and its registered agent for service of summons is Corporation Service Company, 251 Little Falls Drive, Wilmington, DE 19808.

19. Defendant Global Science Research Ltd ("GSR") was incorporated as a private limited company in England on May 29, 2014 and its registered address is 49 Peter Street, 6th Floor, Manchester, England, M2 3NG. It also had offices at Magdalene College, Cambridge, CB3 0AG, United Kingdom.

20. Defendant Aleksandr Kogan is a founding director of Global Science Research Ltd, and now lives in the Bay Area, in Northern California, United States.[8]

21. Defendant SCL Group Limited ("SCL Group"), formerly known as Strategic Communications Laboratories Ltd, is a British company registered with the UK Companies House in 2005.[9] Its headquarters are located at 55 New Oxford Street, London, WC1A 1BS. SCL Group also has multiple U.S. affiliates including SCL Group Inc. with offices in New York located at 597 5th Avenue, 7th Floor, New York, New York, 10036, and SCL USA Inc. with offices in Washington, D.C. located at 1901 Pennsylvania Ave, N.W., Washington, D.C. 20006.

22. SCL Elections Ltd ("SCL Elections") is a British company incorporated on October 17, 2012. Its address is listed as c/o PFK Littlejohn, chartered accountants located at 1 Westferry

[8] https://www.theguardian.com/news/2018/mar/18/facebook-cambridge-analytica-joseph-chancellor-gsr
[9] https://medium.com/@wsiegelman/scl-companies-shareholders-e65a4f394158

Circus, Canary Wharf, London, E14 4HD, UK. Alexander Nix is listed as a director of SCL Elections and the ultimate controlling party as of the end of 2015.[10]

23. SCL USA Inc. ("SCL USA"), is a privately held company incorporated under the laws of the State of Delaware, incorporated on April 22, 2104, and is a wholly owned subsidiary of SCL Elections. Its address is 597 5th Avenue, 7th floor, New York, NY 10017 and its registered agent for service of summons is Erisedentagent, Inc., 1013 Centre Road, Suite 403S, Wilmington, DE 19805. Alexander Nix is listed as the CEO.[11] SCL USA is the alter ego of SCL Group.

24. Defendant Cambridge Analytica LLC ("Cambridge Analytica") is a privately held limited liability company organized under the laws of the State of Delaware, incorporated on December 31, 2013, with its principal offices located at 597 5th Avenue, 7th Floor, New York, NY 10017. Cambridge Analytica also has offices in Washington, D.C. and its registered agent for service of summons is The Corporation Trust Company, 1209 Orange Street, Corporation Trust Center, Wilmington, DE 19801. According to *The Guardian* and *Business Insider,* Steve Bannon was Vice President of Cambridge Analytica from June 2014 until August 2016.[12,13]

25. Defendant Cambridge Analytica Holdings, LLC ("CA Holdings") is a privately held limited liability company organized under the laws of the State of Delaware, incorporated on May 9, 2014. Cambridge Analytica Holdings, LLC's registered agent for service of summons is The Corporation Trust Company, 1209 Orange Street, Corporation Trust Center, Wilmington, DE 19801. According to *The Guardian*, hedge fund billionaire Robert Mercer funded CA Holdings, which created and initially ran Cambridge Analytica.[14]

[10] https://s3-eu-west-1.amazonaws.com/document-api-images-prod/docs/LJ4d6DCFawQ3eIThD55rCIL5Tj_KjkS9pvCsgNx5HcU/application-pdf
[11] https://www.manta.com/c/mh1vpkg/scl-usa-inc
[12] https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
[13] http://www.businessinsider.com/steve-bannon-ties-to-cambridge-analytica-facebook-data-run-deep-2018-3
[14] https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election

26. Defendant Cambridge Analytica Commercial LLC ("CA Commercial") is a privately held limited liability company organized under the laws of the State of Delaware, incorporated on January 21, 2015, and is a division of Cambridge Analytica. CA Commercial's registered agent for service of summons is The Corporation Trust Company, 1209 Orange Street, Corporation Trust Center, Wilmington, DE 19801. Cambridge Analytica is owned in part (19%) by SCL Elections Ltd, a British company owned by SCL Analytics Limited, which is owned in part by Defendant SCL Group.[15] During the relevant time, Alexander Nix was CEO of both SCL Elections Ltd and Cambridge Analytica UK.

27. Defendant Cambridge Analytica Political LLC ("CA Political") is a privately held limited liability company organized under the laws of the State of Delaware, incorporated on January 21, 2015, and is a division of Cambridge Analytica. CA Political's registered agent for service of summons is The Corporation Trust Company, 1209 Orange Street, Corporation Trust Center, Wilmington, DE 19801.

28. Cambridge Analytica, CA Political and CA Commercial all share the same website; https://cambridgeanalytica.org. According to Cambridge Analytica website, CA Political and CA Commercial are Divisions of Cambridge Analytica LLC. Upon information and belief, CA Holdings is a shell holding company for shares of Cambridge Analytica, CA Political and CA Commercial.

29. There is no ownership relationship between Facebook and any Cambridge entity. Further, no Cambridge entity is a party to the contract between Facebook and its users.

[15] https://medium.com/@wsiegelman/scl-companies-shareholders-e65a4f394158

FACTUAL ALLEGATIONS

Facebook's Deceptive Data Collection Platform

30. Millions of Americans who use Facebook have entrusted Facebook to protect their personal data. Facebook expressly assures users that, "You own all of the content and information you post on Facebook, and you can control how it is shared through your privacy and application settings."[16] This representation is false and misleading.

31. Facebook has known for years that its platform could easily and readily be used by third parties to steal users' personal information, that Facebook was not adequately monitoring activities of third-party application developers to whom it had given access to its platform and users' personal information, that users were unaware of the extent of their information Facebook was collecting, and that Facebook was misleading users about the security of their personal information. Sandy Parakilas, the platform operations manager at Facebook responsible for policing data breaches by third-party software developers between 2011 and 2012 stated that he warned senior Facebook executives years ago that its lax approach to data protection risked a major breach. "[M]y concerns" he said, "were that all of the data that left Facebook servers to developers could not be monitored by Facebook, so we had no idea what developers were doing with the data," Parakilas told the Guardian that "Facebook had terms of service and settings that 'people didn't read or understand' and the company did not use its enforcement mechanisms, including audits of external developers, to ensure data was not being misused." "It has been painful watching," he said, "because I know that they could have prevented it."[17]

[16] Facebook Terms of Service, January 30, 2015–present. https://www.facebook.com/terms.php

[17] https://www.theguardian.com/news/2018/mar/20/facebook-data-cambridge- analytica-sandy-parakilas

32. From its inception in 2004, Facebook has built the world's largest social media platform. Facebook now has over two billion monthly active users, with over 200 million in the United States alone. Facebook is now one of the world's leading and most extensive repositories of personal data. The personal information of each of Facebook's users that is regularly recorded and stored in their unique Facebook profiles can include: all manner of biographical information (e.g., current and former names; alternate names; hometown; birthdate; gender; family connections; education; email address; relationship status; education and work history; interests; hobbies; religious and political affiliations; phone number; spoken languages); current and former addresses; dates and times of active sessions on Facebook; dates and times and titles of any advertisements that were "clicked" by the Facebook user; connections with other Facebook users; communications with other Facebook users through the integrated Facebook "Messenger" application and the user Facebook inbox; current and last location; attendance at events and social gatherings; stored credit card information used to make purchases on Facebook; people the Facebook user is "friends" with or follows; Facebook "groups" of which the user is a member; a list of IP addresses that the user has logged into and out of his or her account; posts or sites the user has "liked"; searches conducted by the user on Facebook; photographs and videos documenting all aspects of their lives and the lives of their friends and family; and their activity in Facebook-connected applications ("User Information").

33. Facebook has stated publicly that it collects substantial additional user data across Instagram, Messenger and Whatsapp—three other massive social media/mobile apps it owns.[18] Facebook also admitted that "[m]alicious actors have also abused these features [referring to Facebook's "friend" search functions] to scrape public profile information by submitting phone

[18] https://www.cnbc.com/2018/04/04/facebook-updates-its-terms-of-service-to- include-messenger-instagram.html.

numbers or email addresses they already have through search and account recovery. Given the scale and sophistication of the activity we've seen, we believe most people on Facebook could have had their public profile scraped in this way."

34. A critical feature of the explosive global growth of Facebook is the appearance of control users have over their sensitive User Information. Facebook's privacy settings purport to offer users control over the dissemination of various categories of their User Information, whether it be privately with particular individuals, with all of their Facebook friends, with friends of friends, or with all Facebook users. Users thus reasonably expect User Information will be accessible only to the extent they expressly authorize such access. However, this appearance of control and security is deceptive.

35. The personal information of at least in excess of 80 million Facebook users, including more than 70 million in the U.S. and U.K. was, in fact, outside their control and was accessed, collected, and extracted without their knowledge and consent. By allowing broad, unmonitored access to users' personal information, Facebook enabled the theft of users' personal information by Defendants GSR, Kogan, Cambridge, and SCL Entities and used such personal information to, among other things, improperly target users with advertisements and other communications designed and based upon their own stolen personal information. This was only achievable by Defendants through the unauthorized access to and theft of the vast amount of personal data, including the purportedly private communications among users, collected and maintained by Facebook. Whistleblowers have reported that the stolen data of Facebook users was copied and remains in the hands of third parties.[19] Illegal use of the stolen personal information poses additional far-reaching, high-risk implications for users.

[19] https://www.channel4.com/news/revealed-cambridge-analytica-data-on-thousands-of-facebook-users-still-not-deleted

The Misuse of Stolen Facebook Users' Personal Information by Defendants SCL Entities and Cambridge

36. Cambridge Analytica "is a political analysis firm that claims to build psychological profiles of voters to help its clients win elections."[20] According to its own website, CA Political is "the global leader in data-driven campaigning with over 25 years of experience, supporting more than 100 campaigns across five continents. Within the United States alone, we have played a pivotal role in winning presidential races as well as congressional and state elections."[21] On the commercial side, CA Commercial claims to have "revolutionized the relationship between data and marketing. We combine predictive data analytics, behavioral sciences, and innovative ad tech into one award-winning approach."[22]

37. Christopher Wylie is a former senior employee of Defendant Cambridge Analytica who designed "a plan to harvest the Facebook profiles of millions of people in the U.S., and to use their private and personal information to create sophisticated psychological and political profiles. And then target them with political ads designed to work on their particular psychological makeup."[23]

38. Prior to the formation of Cambridge Analytica, Wylie was "research director across the SCL group, a private contractor that has both defense and elections operations. Its defense arm was a contractor to the UK's Ministry of Defence and the US Department of Defense, among others. Its expertise was in 'psychological operations' – or psyops – changing people's minds not through persuasion, but, instead, through 'informational dominance', a set of techniques that

[20] http://time.com/5205314/facebook-cambridge-analytica-breach/
[21] https://capolitical.com/?__hstc=163013475.cab007272c33dbd1df48f46cdda793ba.1522261580046.1522261580046.1522860395020.2&__hssc=163013475.1.1522860395020&__hsfp=908707084
[22] https://cacommercial.com/?__hstc=163013475.cab007272c33dbd1df48f46cdda793ba.1522261580046.1522261580046.1522860395020.2&__hssc=163013475.2.1522860395020&__hsfp=908707084
[23] https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-faceook-nix-bannon-trump

includes rumor, disinformation and fake news. Wylie's responsibilities included working on contracts the SCL Entities had within the British government to conduct counter-extremism operations in the Middle East, and with the US Department of Defense for work in Afghanistan.

39. In the autumn of 2013, Wylie met Steve Bannon. Mr. Bannon reportedly was told that the SCL entities "do cyberwarfare for elections."[24] Mr. Bannon reportedly introduced Wylie and Alexander Nix, the CEO of the SCL Entities, to Robert and Rebekah Mercer at an in-person meeting in New York. Bannon together with the SCL Entities created one or more of the Cambridge entities. Investor Robert Mercer reportedly provided $15 million in funding for these enterprises. Rebekah Mercer was made President, Mr. Bannon was installed as Vice President and Secretary, and British citizen Alexander Nix became Chief Executive Officer.[25]

The Stealing of Facebook Data

40. On or about June 4, 2014, one month after the formation of CA Holdings, and three years after entry of the FTC Consent Order, SCL Entities through SCL Elections Limited, contracted with Cambridge University psychologist Defendant Aleksandr Kogan and his company Defendant Global Science Research ("GSR") to act as their agent in the creation of an application[26] for use on Facebook ("GSR Application").[27,28] According to whistleblower and former Cambridge employee Christopher Wylie, the purpose of this undertaking was for SCL Entities and Cambridge to gain access to the personal information of both the users who used the application and the Friends of those users.[29] Specifically, according to Time.com, Mr. Wylie claims that "Cambridge

[24] *Id.*
[25] *Id.*
[26] An application is any software program that runs on a computer. https://techterms.com/definition/application
[27] https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election
[28] *See generally* GSR Contract.
[29] *See* Carole Cadwalladr, "'I made Steve Bannon's psychological warfare tool:' meet the data war whistleblower," *The Guardian* (March 18, 2018), https://www.theguardian.com/news/2018/mar/17/data-war-whistleblower-christopher-wylie-facebook-nix-bannon-trump ("Cadwalladr Article")

Analytica's goal was to establish profiling algorithms that would 'allow us to explore mental vulnerabilities of people, then map out ways to inject information into different streams or channels of content online so that people started to see things all over the place that may or may not have been true.'"[30]

41. As reported in The Washington Post, Mr. Wylie also states that this undertaking by SCL Entities and Cambridge was "part of a high-tech form of voter persuasion touted by [Cambridge], which under Bannon identified and tested the power of anti-establishment messages…."[31] The Washington Post also reported that, according to Mr. Wylie, Mr. Bannon, as a top executive of Cambridge Analytica at the time of the data breach in 2014, "was deeply involved in the company's strategy and approved spending nearly $1 million to acquire data, including Facebook profiles, in 2014."[32]

42. Facebook was chosen for several reasons. First, the fact that Facebook's existing developer tools provided application developers with expansive access to both users and their Friends was an "open secret" well known to developers,[33] as well as GSR, Kogan, SCL Entities, and Cambridge.[34]

43. Second, Facebook's Software Development Kit ("SDK") allowed third party developers to add Facebook-related features to their websites or services.[35] These features permitted the developer's service to interact with Facebook in various ways. Among the features

[30] http://time.com/5205314/facebook-cambridge-analytica-breach/
[31] https://www.washingtonpost.com/politics/bannon-oversaw-cambridge-analyticas-collection-of-facebook-data-according-to-former-employee/2018/03/20/8fb369a6-2c55-11e8-b0b0-f706877db618_story.html?utm_term=.9eef8f641a98
[32] *Id.*
[33] *See, e.g.*, Emil Protalinski, *Stalkbook: Stalk Anyone, Even If You're Not Facebook Friends*, CNET (July 23, 2012), https://www.cnet.com/news/stalkbook-stalk-anyone-even-if-youre-not-facebook-friends/.
[34] *See* GSR Contract, at Schedule 2.
[35] An SDK generally refers to a set of software development tools that allow programmers to develop applications that interface with a specific software platform. Here, Facebook's SDK allows Facebook to release code for third party developers to use in order to interact with Facebook's platform.

relevant to this case is the ability to include a "Facebook Login," which let visitors login to a website using their Facebook credentials.

44. When an individual visits or accesses a service utilizing Facebook's SDK, information about the individual's online activities are transmitted back to Facebook. Facebook benefits from this additional information about its users, and the application developer benefits because users can quickly sign in using their Facebook account.

45. Third, Facebook is one of the largest data mining companies in the world, collecting data from over 200 million users just in the United States.[36] With this data, Facebook is uniquely able to provide a holistic picture of a user's online and offline behaviors by linking all of the data it collects on a user's digital conduct with the personal information it extracts from the user's profile and activities.[37]

46. In the second half of 2014, in order to incentivize users to download and access the GSR Application they had developed, SCL Entities and Cambridge, through their agents Kogan and GSR, posed as an academic researcher seeking information through a personality quiz. Kogan "advertised for people who were willing to be paid to take a personality quiz on Amazon's Mechanical Turk and Qualtrics.[38] At the end of which, users gave Kogan's GSR Application, called *thisisyourdigitallife*, permission to access each participant's Facebook profiles."[39] Kogan's GSR Application used Facebook's SDK Facebook Login, meaning that users who wanted to take

[36] Kurt Wagner & Rani Molla, *Facebook Is Not Getting Any Bigger In The United States*, RECODE (March 1, 2018), https://www.recode net/2018/3/1/17063208/facebook-us-growth-pew-research-users ("More than two-thirds of Americans" use Facebook).
[37] Nathan Ingraham, *Facebook Buys Data On Users' Offline Habits For Better Ads*, ENDGAGET (December 30, 2016), https://www.engadget.com/2016/12/30/facebook-buys-data-on-users-offline-habits-for-better-ads/; Cade Metz, *How Facebook Knows When Its Ads Influence Your Offline Purchases*, WIRED (December 11, 2014), https://www.wired.com/2014/12/facebook-knows-ads-influence-offline-purchases/.
[38] Mechanical Turk is an online marketplace where people around the world contract with others to perform various tasks.
[39] *See* Cadwalladr Article.

the personality quiz had to use their Facebook Login credentials to access the quiz, thus giving the developers of the quiz application access to the users' Facebook information.

47. Once the GSR Application was granted access to the profiles and extracting personal information of the users, GSR and Kogan, working on behalf of SCL Entities and Cambridge, and as an agent of SCL Entities and Cambridge, were able to capitalize on Facebook's knowing and willful negligence by accessing the profiles and extracting personal information of all or virtually all of the Friends of the users who participated in the GSR Application personality quiz.

48. Facebook became aware of the data extraction when security protocols were triggered by the massive data download from the GSR Application. According to Facebook, when Facebook investigated the extraction, GSR and Kogan told Facebook the data was to be used for "academic purposes;" Facebook negligently and without verification, accepted this representation and allowed the data extraction to continue.[40] Specifically, according to Facebook, it was told by GSR and Kogan, that

> This app is part of a research program in the Department of Psychology at the University of Cambridge. We are using this app for research purposes – learning about how people's Facebook behavior can be used to better understand their psychological traits, well-being, health, etc and overcome classic problems in social science. Users of the app will be presented with a description of the types of data we gather and the scientific purpose of the data. Users will be informed that the data will be carefully protected and never used for commercial purposes.[41]

49. Facebook claims that the first time it learned that the data extraction had not been for academic use was later in time: when the Guardian published its report about the SCL Entities

[40] Chloe Aiello, *Developer Behind The App At The Center Of Data Scandal Disputes Facebook's Story*, CNBC (March 21, 2018), https://www.cnbc.com/2018/03/21/aleksander-kogan-facebook-shouldve-known-how-app-data-was-being-used html.
[41] *Id.*

and Cambridge acquiring and utilizing the extracted Facebook data in December 2015.[42] However, even when faced with the possibility of such a violation of its policies in December of 2015, Facebook negligently failed to take any remedial action and waited for several months, until August of 2016, before taking any action. Even then all that Facebook did was send Cambridge a letter.[43] In August 2016, Facebook wrote to Christopher Wylie, who had left Cambridge in 2014, informing him "that the data had been illicitly obtained and that '[Kogan's company] was not authorized to share or sell it,' stating that the extracted data must be deleted immediately.[44,45]

50. According to Wylie, by August of 2016, there were multiple copies of the extracted data, and that it had been emailed to a number of recipients unencrypted. He states that Facebook made no efforts thereafter to either retrieve the extracted data or confirm that he, or any other recipient, had deleted it.[46]

51. While GSR, Kogan, SCL Entities and Cambridge now claim that they "clearly stated that users were granting us the right to use the data in broad scope, including selling and licensing data..."[47], the contemporaneous written statements in the letter sent to Facebook is directly contrary to this purported representation.

52. While a Facebook spokesperson made an unsupported, contradictory statement that "[b]oth Aleksandr Kogan as well as the SCL Group and [Cambridge] certified to us that they destroyed the data in question," Mark Zuckerberg, Facebook's CEO, admitted that *"[t]his was a major breach of trust, and I'm really sorry this happened. You know, we have a basic responsibility*

[42] Ben Jacobs, *Ted Cruz using firm that harvested data on millions of unwitting Facebook users*," The Guardian (December 11, 2015), https://www.theguardian.com/us-news/2015/dec/11/senator-ted-cruz-president-campaign-facebook-user-data.
[43] *Id.*
[44] Cadwalladr Article
[45] *See* Letter from Facebook to C. Wylie, attached hereto as Exhibit 2 ("Facebook Letter").
[46] *Id.*
[47] *Id.*

to protect people's data and if we can't do that then we don't deserve to have the opportunity to serve people."[48]

53. This admission by Mr. Zuckerberg acknowledges that Facebook knew it had a clear duty to protect the personal information of its users, and in fact, had a clear duty to protect the personal information of its users, and that it breached that duty in several ways, including; its failure to prevent the unauthorized extraction of information from occurring by correcting and eliminating a known weakness in its developer platform; its failure to use the means it had to adequately protect the information; its failure to retrieve the information immediately upon discovery of its unauthorized extraction; and its failure to inform Facebook users in a timely manner.

54. Moreover, Mr. Zuckerberg's admission that Facebook breached its duties is confirmed by a review of Facebook's policies in place at the time. Specifically, Facebook's "Data Use Policy," effective at the time that GSR, Kogan, SCL Entities, and Cambridge accessed and extracted the data, states in part:

> **How we use the information we receive**: We use the information we receive about you in connection with the services and features we provide to you and other users like your friends, our partners, the advertisers that purchase ads on the site, and the developers that build the games, applications, and websites you use. For example, in addition to helping people see and find things that you do and share, we may use the information we receive about you:
>
> - *as part of our efforts to keep Facebook products, services and integrations safe and secure;*
> - *to protect Facebook's or others' rights or property;*
> - to provide you with location features and services, like telling you and your friends when something is going on nearby;
> - to measure and understand the effectiveness of ads you and others see, including to deliver relevant ads to you;
> - to make suggestions to you and other users on Facebook, such as: suggesting that your friend use our contact importer because you found

[48] *See* Danielle Wiener-Bronner, "Mark Zuckerberg has regrets: 'I'm sorry that this happened'" CNN (March 21, 2018), http://money.cnn.com/2018/03/21/technology/mark-zuckerberg-apology/index.html.

> friends using it, suggesting that another user add you as a friend because the user imported the same email address as you did, or suggesting that your friend tag you in a picture they have uploaded with you in it; and
> - for internal operations, including troubleshooting, data analysis, testing, research and service improvement. (emphasis added)[49]

55. Facebook's "Data Use Policy" also stated:

> While you are allowing us to use the information we receive about you, you always own all of your information. *Your trust is important to us*, which is why we don't share information we receive about you with others unless we have:
> - received your permission;
> - given you notice, such as by telling you about it in this policy; or
> - removed your name and any other personally identifying information from it. (emphasis added).[50]

56. The Federal Trade Commission issued guidance on how to appropriately respond to data breaches, entitled "Data Breach Response: A Guide for Business," in which it advises, "When your business experiences a data breach, notify law enforcement, other affected businesses, and affected individuals."[51] Facebook failed to follow this FTC guidance once it was released, instead choosing to keep this massive data breach by Cambridge a secret from its affected users until it was forced to admit that the breach had occurred, and only when it was made public by third parties.

57. Several things are clear. First, GSR, Kogan, SCL Entities, and Cambridge, either directly or through their affiliated corporate entities and/or agents, mislead Facebook regarding their true purposes and goals behind the development and execution of the *thisisyourdigitallife* GSR Application.

58. Second, GSR, Kogan, SCL Entities and Cambridge, either directly or through their affiliated corporate entities and/or agents, did not disclose to Facebook that they were using and/or

[49] *Data Use Policy*, Facebook, Inc. (Date of Last Revision: November 15, 2013), https://www.facebook.com/full_data_use_policy.
[50] *Id.*
[51] FEDERAL TRADE COMMISSION, "Data Breach Response: A Guide for Business" (2016)

had used the GSR Application as a vehicle, through the voluntary participants who they incentivized to take the quiz, to improperly gain access to, collect and extract the personal information from approximately 71.6 million Facebook users who did not access the GSR Application or otherwise consent to such an intrusion, theft and use.

59. Third, Facebook negligently failed to properly inquire or investigate what information GSR, Kogan, SCL Entities and/or Cambridge were accessing, collecting, and extracting.

60. Fourth, Facebook knowingly failed to take action to eliminate a "backdoor" that allowed applications created using its developer platform to be portals through which third parties have obtained widescale, unauthorized access to the information of tens of millions of Facebook users.

61. Fifth, Facebook knowingly failed to comply with its obligations as set forth on its website and provided to each of its Facebook users.

62. Sixth, Facebook negligently failed to adequately protect its users' information contrary to its obligations set forth the 2011 Consent Order entered into between Facebook and the FTC, discussed *infra*.

63. Seventh, Facebook, upon learning of the unauthorized extraction of users' information and Cambridge's gross invasion of privacy, withheld from its users knowledge of that wrongdoing, as well as knowingly and/or negligently refusing to take adequate steps to ensure the return and/or destruction of the stolen information.

2011 FTC Investigation of Facebook

64. Prior to GSR's, Kogan's, SCL Entities' and Cambridge's development and execution of the *thisisyourdigitallife* application, in 2011, as a result of an investigation, the

Federal Trade Commission prepared a draft complaint against Facebook, alleging violations of the Federal Trade Commission Act. Specifically, the FTC alleged, *inter alia*, that Facebook's platform allowed third parties to "develop, run, operate software applications, such as games, that users can interact with online ("Platform Applications")."[52]

65. According to the FTC, these Platform Applications enabled access to a user's personal information in one of two ways; (a) if the user authorized the access directly; or (b) if a user's Facebook Friend authorizes the Platform Application. In the latter case, the Platform Application gains access to at least some of a Facebook user's information even though the user has not authorized the Platform Application to do so.[53]

66. Further, the FTC alleged that, despite whatever Facebook privacy settings a user selected, "a user's choice to restrict profile information to "Only Friends," or "Friends of Friends" would be ineffective as to certain third parties."[54] In fact, "Facebook has made profile information that a user chose to restrict to "Only Friends" or "Friends of Friends" accessible to any Platform Applications that the user's Friends may have used ("Friends' Apps").[55]

67. The FTC acknowledged that it was possible for a user to click on a link for "Applications," "Apps," or "Applications and Websites" in order to reach a different page containing "Friends' App Settings," which would allow users to restrict the information that a Friends' App could access. But it is also alleged that "in many instances, the links to "Applications," "Apps," or "Applications and Websites" have failed to disclose that a user's choices made through Profile Privacy Settings have been ineffective against Friends' Apps. For

[52] *In the Matter of Facebook, Inc., a corporation*, U.S. Federal Trade Commission Complaint ("FTC Complaint"), at ¶ 4.
[53] *Id.*, at ¶ 9.
[54] *Id.*, at ¶ 14.
[55] *Id.*

example, the language alongside the Applications link … has stated '[c]ontrol what information is available to applications ***you use*** on Facebook." (emphasis added)[56]

68. The FTC asserted that Facebook's representation that "through their Profile Privacy Settings, users can restrict access to their profile information to specific groups, such as "Only Friends" or "Friends of Friends" was false or misleading.[57]

69. Privacy concerns were not a new phenomenon to Facebook. On December 8, 2009, Facebook started to implement a new privacy policy which designated certain user information as "publicly available," including their name, profile picture, gender, Friend list, pages, and networks. Facebook's implementation prevented users from restricting access to this information through their Profile Privacy Settings, and all of their prior privacy settings relating to this information were overridden.[58]

70. In Count 3 of its Complaint, the FTC asserted that "Facebook materially changed its promises that users could keep such information private. Facebook retroactively applied these changes to personal information that it had previously collected from users, without their informed consent, in a manner that has caused or has been likely to cause substantial injury to consumers…."[59] Therefore, the FTC has recognized that there is an inherent or intrinsic value associated with the ability to control who has access to certain kinds of personal information, and that the unauthorized access and/or use of such information causes substantial injury to the individual whose information is improperly revealed and/or used.

71. In Count 4, the FTC charged that Facebook made repeated public statements to the effect that the scope of Platform Applications' access to a user's data was limited to only that

[56] *Id.* at ¶¶ 15-16.
[57] *Id.* at Count 1, ¶¶ 17-18.
[58] *Id.* at ¶¶ 19-22.
[59] *Id.* at Count 3, ¶ 29.

information needed for the application to work or operate. Contrary to these statements, however, "from approximately May 2007 until July 2010, in many instances, Facebook has provided Platform Applications unrestricted access to user profile information that such Applications have not needed to operate," rendering Facebook's statements, "false and misleading representation[s]."[60]

72. In response to the FTC's investigation and to resolve the serious issues raised by the FTC's Complaint, Facebook entered into the FTC Consent Order on or about November 29, 2011.[61]

73. The FTC Consent Order contained a requirement prohibiting Facebook from making any misrepresentations about several topics, including "its collection or disclosure of any covered information;" "the extent to which a consumer can control the privacy of any covered information maintained by [Facebook];" "the extent to which [Facebook] makes or has made covered information accessible to third parties;" and "the steps [Facebook] takes or has taken to verify the privacy or security protections that any third party provides…."[62]

74. However, more relevant here, are the FTC Consent Order's requirements related to Facebook's sharing of a user's nonpublic information. Specifically, the FTC ordered, and Facebook agreed, that:

> It is Further Ordered that [Facebook] and its representatives, in connection with any product or service, in or affecting commerce, prior to any sharing of a user's nonpublic user information by [Facebook] with any third party, which materially exceeds the restrictions imposed by a user's privacy setting(s), shall: (A) clearly and prominently disclose to the user, separate and apart from any "privacy policy," "data use policy," "statement of rights and responsibilities" page, or other similar document: (1) the categories of nonpublic user information that will be disclosed to such third parties, (2) the identity or specific categories of such third parties, and

[60] *Id.* at ¶¶ 30-33.
[61] *See, generally,* FTC Consent Order.
[62] FTC Consent Order, at Section I.A.D.

> (3) that such sharing exceeds the restrictions imposed by the privacy setting(s) in effect for the user; and (B) obtain the user's affirmative express consent.[63]

75. Therefore, no later than November 2011, Facebook was aware that third parties could access the personal information of users through applications on Facebook in which users themselves had not participated. Such access, collection, and extraction of personal information was available so long as any one of a multitude of a user's Friends had participated in the application. The fact that Facebook's existing developer tools provided such access was an open secret well known to developers.[64] Further, Facebook was aware that providing such unauthorized access to a user's personal information would cause that user substantial injury.

76. Despite this knowledge and its obligations to its users, Facebook took no affirmative action, and, thereby, refused or otherwise failed to fix, change, or otherwise remedy this known defect in its existing developer tools. As a result, GSR and Aleksandr Kogan, working with SCL Entities and Cambridge, were able to utilize this defect and capitalize on this unauthorized access through the use of the *thisisyourdigitallife* GSR Application. As described above, approximately 270,000 U.S. Facebook users installed and participated in the GSR Application, providing GSR, Kogan, the SCL Entities, and Cambridge access, not only to the personal information of those 270,000 participants, but also unauthorized access to the theft of the personal information of approximately 71.6 million U.S. Facebook users who were Friends of the 270,000 participants, causing substantial injury to the 71.6 million individuals.

[63] *Id.* at Section II.A. and II.B.
[64] *See, e.g.*, Emil Protalinski, *Stalkbook: Stalk Anyone, Even If You're Not Facebook Friends*, CNET (July 23, 2012), https://www.cnet.com/news/stalkbook-stalk-anyone-even-if-youre-not-facebook-friends/.

CLASS ACTION ALLEGATIONS

77. Pursuant to Rule 23(b)(2) and (b)(3) of the Federal Rules of Civil Procedure, Plaintiffs, individually and on behalf of all others similarly situated, bring this lawsuit on behalf of themselves and as a class action on behalf of the following class:

> All natural persons who registered for Facebook accounts in the United States or the United Kingdom, who did not utilize, download, or otherwise access the *yourdigitallife* GSR Application and whose Personal Information was obtained from Facebook by Defendants GSR, Kogan, SCL Entities and/or Cambridge, either directly or indirectly, without authorization or in excess of authorization.

78. Excluded from the Class are any entities, including Defendants, and Defendants' officers, agents, and employees. Also excluded from the Class are counsel for Plaintiffs, the judge assigned to this action, and any member of the judge's immediate family.

A. Numerosity

79. The first requirement of Rule 23(a) is met when "the class is so numerous that joinder of all members is impractical." Fed. R. Civ. P. 23(a)(1). Generally, the numerosity requirement is met when the class comprises 40 or more members. *Hayes v. Wal-Mart Stores, Inc.*, 725 F.3d 349, 357 n.5 (3d Cir. 2013); *Nat'l Fed'n of the Blind v. Target Corp.*, 582 F. Supp. 2d 1185, 1199 (N.D. Cal. 2007) ("As a general rule, classes numbering greater than 41 individuals satisfy the numerosity requirement."). Numerosity in this case is easily satisfied. The members of the Class are so numerous that joinder of all members of any Class would be impracticable. Plaintiffs reasonably believe that Class members number seventy-one point six (71.6) million people or more in the aggregate. The names and addresses of Class members are identifiable through documents maintained by Defendants.

B. Commonality and Predominance

80. Rule 23(a)(2) requires that "there are questions of law or fact common to the class." To meet the commonality requirement, Plaintiffs must demonstrate that the proposed class members "have suffered the same injury." *Wal-Mart Stores, Inc. v. Dukes*, 131 S. Ct. 2541, 2551 (2011) (quoting *Gen. Tel. Co. of Sw. v. Falcon*, 457 U.S. 147, 157 (1982)). In other words, commonality requires that the claims of the class "depend on a common contention…of such a nature that it is capable of class-wide resolution – which means that determination of its truth or falsity will resolve an issue that is central to the validity of each one of the claims in one stroke." *Id*. Commonality may be shown when the claims of all class members "depend upon a common contention" and "even a single common question will do." *Dukes*, 131 S. Ct. at 2545, 2556. This action involves common questions of law or fact, which predominate over any questions affecting individual Class members, including:

a. Whether Facebook represented that it would safeguard Plaintiffs' and Class Members' Personal Information and not disclose it without consent;

b. Whether GSR, Kogan, SCL Entities and Cambridge Defendants and/or their agents improperly obtained Plaintiffs' and Class Members' Personal Information without authorization or in excess of any authorization;

c. Whether Facebook was aware of GSR's, Kogan's, SCL Entities' and Cambridge Defendants' and/or their agents' improper access to, collection of, and extraction of Plaintiffs' and Class Members' Personal Information;

d. Whether Facebook owed a legal duty to Plaintiffs and the Class to exercise due care in collecting, storing, safeguarding, obtaining, and/or providing access to their Personal Information;

e. Whether Facebook breached a legal duty to Plaintiff and the Class to exercise due care in collecting, storing, safeguarding, and/or obtaining their Personal Information;

f. Whether Class Members' Personal Information was improperly and/or illegally obtained by GSR, Kogan, SCL Entities and Cambridge Defendants and/or their agents;

g. Whether Defendants' conduct violated the SCA, 18 U.S.C. §§ 2701, *et seq.*;

h. Whether Plaintiffs and the Class are entitled to equitable relief, including, but not limited to, injunctive relief, restitution, and disgorgement; and

i. Whether Plaintiffs and the other Class Members are entitled to actual, statutory, consequential, punitive or other forms of damages, and other monetary relief.

81. Defendants engaged in a common course of conduct giving rise to the legal rights sought to be enforced by Plaintiffs individually and on behalf of the Members of the Class. Similar or identical statutory and common law violations, business practices, and injuries are involved. Individual questions, if any, pale by comparison, in both quantity and quality, to the numerous common questions that dominate this action.

C. Typicality

82. Typicality requires that Plaintiffs' claims be typical of other Class Members. Fed. R. Civ. P. 23(a)(3). While the typicality inquiry focuses on the similarity between the named Plaintiffs' legal and remedial theories and the theories of those whom they purport to represent, it does not require that all Class Members have identical claims. *In re Yahoo Mail Litig.*, 308 F.R.D. 577, 593 (N.D. Cal. 2015); *Grossmann v. First Pennsylvania Corp.*, 1991 U.S. Dist. LEXIS 15373, *9 (E.D. Pa. Oct. 23, 1991). The purpose of the typicality requirement is to ensure that the Class Representatives' interests are "sufficiently similar to the rest of the class – in terms of their legal claims, factual circumstances, and stake in the litigation – so that certifying those individuals to

represent the class will be fair to the rest of the proposed class." *In re Schering Plough Corp. ERISA Litig.*, 589 F.3d 585, 597 (3rd Cir. 2009); *In re Yahoo Mail Litig.*, 308 F.R.D. at 593 ("Typicality is satisfied 'when each class member's claim arises from the same course of events, and each class member makes similar legal arguments to prove the defendants' liability.'") (quoting *Rodriguez v. Hayes*, 591 F.3d 1105, 1124 (9th Cir. 2010).). *See, e.g., Neal v. Casey*, 43 F.3d 48, 58 (3rd Cir. 1994) (noting that "cases that challenge the same unlawful conduct which affects both the named plaintiffs and the putative class usually satisfy the typicality requirement irrespective of the varying fact patterns underlying the individual claims.")

83. Plaintiffs' claims are typical of the claims of the other members of the Class because, among other things, Plaintiffs and the other Class Members were injured through the substantially uniform misconduct by Defendants. Plaintiffs are advancing the same claims and legal theories on behalf of themselves and all other Class Members, and there are no defenses that are unique to Plaintiffs. The claims of Plaintiffs and those of other Class Members arise from the same operative facts and are based on the same legal theories.

D. Adequacy of Representation

84. Rule 23(a) requires that the representative parties have and will continue to "fairly and adequately protect the interests of the class." Fed. R. Civ. P. 23(a)(4). Both the Ninth and Third Circuits have adopted a two-part test for this element, requiring both that "(a) the plaintiff's attorney must be qualified, experienced, and generally able to conduct the proposed litigation, and (b) the plaintiff must not have interests antagonistic to those of the class." *Wetzel v. Liberty Mutual Ins. Co.*, 508 F.2d 239, 247 (3rd Cir. 1975), *cert. denied*, 421 U.S. 1011 (1975); *see also Hanlon v. Chrysler Corp.*, 150 F.3d 1011, 1020 (9th Cir. 1998); *In re Juniper Networks Sec. Litig*., 264

F.R.D. 584, 590 (N.D. Cal. 2009); *Cristiano v. Courts of Justices of the Peace*, 115 F.R.D. 240, 248 (D. Del. 1987).

85. Plaintiffs are adequate representatives of the class because their interests do not conflict with the interests of the other Class Members they seek to represent; they have retained counsel competent and experienced in complex class action litigation and Plaintiffs will prosecute this action vigorously. The Class Members' interests will be fairly and adequately protected by Plaintiffs and their counsel.

E. Superiority and Predominance

86. A class action may be maintained under Rule 23(b)(3) if all Rule 23(a) requirements are met and "the court finds that the questions of law or fact common to class members predominate over any questions affecting only individual members, and that a class action is superior to other available methods for fairly and efficiently adjudicating the controversy."[65] *See Amchem Prods., Inc. v. Windsor*, 521 U.S. 591, 615-616 (1997) (addressing predominance and superiority requirements). The predominance inquiry "tests whether proposed classes are sufficiently cohesive to warrant adjudication by representation." *Id.* at 623.

87. The superiority requirement "asks the court to balance, in terms of fairness and efficiency, the merits of a class action against those of alternative available methods of adjudication." *In re NFL Players Concussion Injury Litig*., 821 F.3d 410, 434 (3rd Cir. 2016) (quoting *Warfarin Sodium Antitrust Litig.*, 391 F.3d 516, 533-34 (3rd Cir. 2004).) A class action is superior where "'the rights of groups of people who individually would be without effective strength to bring their opponents into court at all.'" *Datta v. Asset Recovery Solutions, LLC*, 2016

[65] Pertinent matters include: (1) the class members' interests in individually controlling the prosecution or defense of separate actions; (2) the extent and nature of any litigation concerning the controversy already begun by or against class members; (3) the desirability or undesirability of concentrating the litigating the claims in the particular forum; and (4) the likely difficulties in managing a class action. Fed. R. Civ. P. 23(b)(3)(A)-(D).

U.S. Dist. LEXIS 36446, *29 (N.D. Cal. March 18, 2016) (quoting *Amchem Prods. v. Windsor*, 521 U.S. 591, 617 (1997).) Class actions are particularly appropriate where, as here, "it is necessary to permit the plaintiffs to pool claims which would be uneconomical to litigate individually." *Phillips Petroleum Co. v. Shutts*, 472 U.S. 797, 809 (1985).

88. A class action is superior to any other available means for the fair and efficient adjudication of this controversy, and no unusual difficulties are likely to be encountered in the management of this matter as a class action. The damages, harm, or other financial detriment suffered individually by Plaintiffs and the other Class Members are relatively small, if any, compared to the burden and expense that would be required to litigate their claims on an individual basis against Defendants, making it impracticable for Class Members to individually seek redress for Defendants' wrongful conduct. Even if Class Members could afford individual litigation, the court system could not. Individualized litigation would create a potential for inconsistent or contradictory judgments and increase the delay and expense to all parties and the court system. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication economies of scale, and comprehensive supervision by a single court.

89. Further, Defendants have acted or failed to act on grounds generally applicable to the Class, and accordingly, final injunctive or corresponding declaratory relief regarding the Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

90. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

a. Whether Class Members' Personal Information was obtained by GSR, SCL Entities and Cambridge Defendants and/or their agents;

b. Whether (and when) Facebook knew about the improper collection and theft of Personal Information;

c. Whether Defendants' conduct violated the SCA, 18 U.S.C. §§ 2701, *et seq.*;

d. Whether Facebook's representations that they would secure and not disclose, without consent, the Personal Information of Plaintiffs and Class Members were facts that reasonable persons could be expected to rely upon when deciding whether to use Facebook's services;

e. Whether Facebook misrepresented the safety of its many systems and services, specifically the security thereof, and their ability to safely store Plaintiffs' and Class Members' Personal Information;

f. Whether Facebook failed to comply with its own policies and applicable laws, regulations, the FTC Consent Judgment, and industry standards relating to data security;

g. Whether Facebook failed to meet its obligations under the User Terms of Service;

h. Whether Defendants' acts, omissions, misrepresentations, and practices were and are likely to deceive consumers;

i. Whether Facebook failed to adhere to its posted privacy policy concerning the care it would take to safeguard and protect Class Members' Personal Information; and

j. Whether Facebook negligently and materially failed to adhere to its posted privacy policy with respect to the extent of its disclosure of users' Personal Information.

CAUSES OF ACTION

Claim I: Violation of the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq*. Against GSR, Kogan, SCL Entities and Cambridge

91. Plaintiffs hereby adopt by reference each and every preceding paragraph stated in this Complaint as if fully set forth herein.

92. The Stored Communications Act ("SCA") allows a private right of action against anyone who "(1) intentionally accesses without authorization a facility through which an electronic communication service is provided; or (2) intentionally exceeds an authorization to access that facility; and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage in such system." *See* 18 U.S.C. § 2701(a); *see also* 18 U.S.C. § 2707(a) (cause of action).

93. The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*, defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce …." 18 U.S.C. § 2510(12). The SCA incorporates this definition of "electronic communication."

94. To create the information transferred to Facebook such as all posts, private messages, and similar communication (collectively "Facebook content"), Facebook users transmit writing, images, or other data via the Internet from their computers or mobile devices to Facebook's servers. This Facebook content, therefore, constitutes electronic communications for purposes of the SCA.

95. The SCA defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Facebook content is transmitted via an electronic communication service

because Facebook provides its users with the ability to send or receive wire or electronic communications, including private messages and wall posts. Facebook, therefore, is an electronic communication service provider for purposes of the SCA.

96. The SCA distinguishes between two types of electronic storage. The first is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof." 18 U.S.C. § 2510(17)(A). The second type is defined as "any storage of such communication by an electronic communication for purposes of backup protection of such communication." 18 U.S.C. § 2510(17)(B). Because Facebook saves and archives Facebook content indefinitely, Facebook content is stored in electronic storage for purposes of the SCA.

97. Facebook allows users to select privacy settings for their Facebook content. Access can be limited to a user's Facebook friends, to particular groups or individuals, or to just the particular Facebook user. When users make Facebook content inaccessible to the general public, the information is considered private for purposes of the SCA.

98. Defendants GSR, Kogan, SCL Entities and Cambridge have violated 18 U.S.C. § 2701(a) because they intentionally accessed, either directly or indirectly through an agent, Plaintiffs' information and/or intentionally exceeded their authorization to access Plaintiffs' information and, in so doing, obtained unauthorized access to an electronic communication while in electronic storage.

99. Defendants GSR, Kogan, SCL Entities and Cambridge had actual knowledge of, and benefitted from, this practice including the gain of monetary profits.

100. As a result of Defendants' conduct described herein and its violations of § 2701, Plaintiffs and the Class have suffered actual injury in the form of dissemination of private

information, loss of sales value of private information, costs of mitigation for the disclosure, loss of the benefit of the bargain as a Facebook user by excess disclosure of private information necessary to use the Facebook service, and emotional distress.

101. Plaintiffs, on behalf of themselves and the Class, seek an order enjoining Defendants' conduct and are entitled to the greater of their actual damages or statutory damages of $1,000 per violation, as well as disgorgement, punitive damages, attorneys' fees, and costs. 18 U.S.C. § 2707(c)

Claim II: Violation of the Stored Communications Act, 18 U.S.C. §§ 2701, *et seq.* Against Facebook

102. Plaintiffs hereby adopt by reference each and every preceding paragraph stated in this Complaint as if fully set forth herein.

103. The Stored Communications Act ("SCA") allows a private right of action against "a person or entity providing an electronic communication service to the public" who "knowingly divulge(s) to any person or entity the contents of a communication while in electronic storage by that service." *See* 18 U.S.C. § 2702(a)(1); *see also* 18 U.S.C. § 2707(a) (cause of action).

104. The Electronic Communications Privacy Act, 18 U.S.C. §§ 2510, *et seq.*, defines an "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce …." 18 U.S.C. § 2510(12). The SCA incorporates this definition of "electronic communication."

105. To create the information transferred to Facebook such as all posts, private messages, and similar communication (collectively "Facebook content"), Facebook users transmit writing, images, or other data via the Internet from their computers or mobile devices to

Facebook's servers. This Facebook content, therefore, constitutes electronic communications for purposes of the SCA.

106. The SCA defines "electronic communication service" as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15). Facebook content is transmitted via an electronic communication service because Facebook provides its users with the ability to send or receive wire or electronic communications, including private messages and wall posts. Facebook, therefore, is an electronic communication service provider for purposes of the SCA.

107. The SCA distinguishes between two types of electronic storage. The first is defined as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof." 18 U.S.C. § 2510(17)(A). The second type is defined as "any storage of such communication by an electronic communication for purposes of backup protection of such communication." 18 U.S.C. § 2510(17)(B). Because Facebook saves and archives Facebook content indefinitely, Facebook content is stored in electronic storage for purposes of the SCA.

108. Facebook allows users to select privacy settings for their Facebook content. Access can be limited to a user's Facebook friends, to particular groups or individuals, or to just the particular Facebook user. When users make Facebook content inaccessible to the general public, the information is considered private for purposes of the SCA.

109. Defendant Facebook is a "person or entity providing an electronic communication service to the public" as set forth by the SCA, meaning that Facebook's content is covered by the SCA. *Ehling v. Monmouth-Ocean Hospital Service*, 961 F. Supp. 2d 659, 666 (D.N.J. 2013). Defendant Facebook has itself conceded and recognized that the SCA was enacted by Congress to

address access to stored electronic communications such as those on Facebook's platform. *Campbell v. Facebook Inc.*, 77 F. Supp. 3d 836, 840-41 (N.D. Cal. 2014).

110. Facebook knowingly allowed Defendants GSR, Kogan, SCL Entities and Cambridge, directly or indirectly, through the creation of an application as a developer, to improperly access the Facebook content or Personal Information of 71.6 million registered Facebook users without their knowledge or consent.

111. Defendant Facebook has violated 18 U.S.C. § 2702(a) because it knowingly divulged to GSR, SCL Entities and Cambridge, either directly or indirectly, the contents of a communication while in Facebook's electronic storage through the creation of an application as a developer.

112. Defendant Facebook had actual knowledge of, and benefitted from, this practice including the gain of monetary profits.

113. As a result of Defendants' conduct described herein and its violations of § 2702, Plaintiffs and the Class have suffered actual injury in the form of dissemination of private information, loss of sales value of private information, costs of mitigation for the disclosure, loss of the benefit of the bargain as a Facebook user by excess disclosure of private information necessary to use the Facebook service, and emotional distress.

114. Plaintiffs, on behalf of themselves and the Class, seek an order enjoining Defendant's conduct and are entitled to the greater of their actual damages or statutory damages of $1,000 per violation, as well as disgorgement, punitive damages, attorneys' fees, and costs. 18 U.S.C. § 2707(c)

Claim III: Negligence And Willful Negligence Against Facebook

115. Plaintiffs hereby adopt by reference each and every preceding paragraph stated in this Complaint as if fully set forth herein.

116. Defendant Facebook had a duty to protect the privacy and personal information of its users.

117. Defendant Facebook had a duty to comply with the requirements set forth in the FTC Consent Order.

118. Defendant Facebook breached those duties when it allowed third parties access to its users' Personal Information, when it failed to take adequate remedial measures to protect users' Personal Information, and when it failed to notify its users of the data breach. Defendant Facebook's negligence constituted a willful and conscious disregard of the rights of Plaintiffs and the Class Members when it, with knowledge of the high and unacceptable risk of the means of unauthorized data access and the known ability to eliminate such means, declined and/or refused to take such measures and utilize such known means to adequately protect users' Personal Information.

119. Defendant Facebook's allowing third parties to access its users' Personal Information, failure to take adequate remedial measures to protect users' Personal Information, and failure to notify its users of the data breach caused Plaintiffs' and Class Members harm because users' privacy rights were violated and they lacked adequate notice to protect themselves and their privacy interests.

Claim IV: Fraud Against Facebook

120. Plaintiffs hereby adopt by reference each and every preceding paragraph stated in this Complaint as if fully set forth herein.

121. Facebook, as part of the Consert Order, made public assurances to the Plaintiffs and Class Members that Facebook would take steps to prevent disclosure of nonpublic user information to any third party without, among other things, first obtaining the users' affirmative consent. At the time of this public announcement, Facebook knew that third parties could access the personal information of users through applications that users themselves had not given access to, e.g., if the users' Friends had granted a third-party application access. At the time it made the public commitments in the Consent Order, Facebook did not intend to stop that means of access as evidenced by its failure to make any such changes to its platform. As a result, Facebook's assurances in the Consent Order were false and misleading.

122. This misrepresentation was material. The FTC deemed disclosure of nonpublic information of Facebook users without consent to be significant enough to sue Facebook for that action. Further, upon information and belief Facebook knew that this access to personal information of an unknowing user would cause that user substantial injury.

123. Plaintiffs and the Class Members were entitled to, and in fact did, rely on Facebook's misrepresentations. This reliance was detrimental to Plaintiffs and the Class Members. For example, Facebook's misrepresentations gave Plaintiffs and the Class Members a false sense of security regarding access to their respective nonpublic information that was in Facebook's possession. This reliance enabled GSR's, SCL Entities' and Cambridge's acquisition of Plaintiffs' and the Class Members' nonpublic information, which caused Plaintiffs and the Class Members to suffer damages in an amount to be proved at trial.

124. Plaintiffs and the Class Members are entitled to recover punitive damages as a result of Facebook's fraudulent conduct.

Claim V: Fraud Against GSR, Kogan, SCL Entities and Cambridge

125. Plaintiffs hereby adopt by reference each and every preceding paragraph stated in this Complaint as if fully set forth herein.

126. GSR, SCL Entities and Cambridge's agent, misrepresented both the purpose of and authorization for GSR's, Kogan's, SCL Entities' and Cambridge's data pull from Facebook of nonpublic user information, including that of Plaintiffs and the Class Members.

127. Facebook, relying on these misrepresentations, permitted GSR, Kogan, SCL Entities, and Cambridge to complete the illegal data pull. Although GSR, Kogan, SCL Entities, and the Cambridge entities directed their misrepresentations at Facebook, Plaintiffs and the Class Members – specifically their nonpublic information – were the actual targets of GSR's, Kogan's, SCL Entities' and Cambridge's fraudulent plan. GSR's, Kogan's, SCL Entities', and Cambridge's misrepresentations were material; the misrepresentations enabled GSR, Kogan, SCL Entities and Cambridge to access nonpublic information of 71.6 million Facebook users, including Plaintiffs and the Class Members, for which GSR, Kogan, SCL Entities, and Cambridge lacked authorization and/or consent.

128. GSR's, Kogan's, SCL Entities', and Cambridge's fraudulent acquisition of Plaintiffs' and the Class Members' nonpublic information caused Plaintiffs and the Class Members to suffer damages in an amount to be proven at trial.

129. Plaintiffs and the Class Members are entitled to recover punitive damages as a result of GSR's, Kogan's, SCL Entities', and Cambridge's fraudulent conduct.

JURY DEMAND

Plaintiffs assert their rights under the Seventh Amendment to the U.S. Constitution and demands, in accordance with Federal Rules of Civil Procedure 38, a trial by jury on all issues.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs, individually and on behalf of the putative Class Members, respectfully prays that the Court enter an order: (a) certifying the United States Class and appointing Plaintiffs as Class Representatives; (b) finding that Facebook's conduct violated the Store Communications Act; (c) finding that GSR's, Kogan's, SCL Entities', and Cambridge's conduct violated the Store Communications Act; (d) finding that Facebook's conduct breach its agreements with Plaintiffs and the Class Members; (e) finding that Facebook's conduct was negligent; (f) finding that Facebook's negligence constituted a willful and conscious disregard of the rights of Plaintiffs and the Class Members under Cal. Civ. Code § 3294 and common law; (g) finding that Facebook committed fraud on Plaintiffs and the Class Members; (h) finding that GSR, Kogan, SCL Entities, and Cambridge committed fraud on Facebook that damaged Plaintiffs and the Class Members; (i) enjoining all Defendants from engaging in further negligent and unlawful business practices; (j) awarding Plaintiffs and the Class Members nominal, actual, compensatory, and consequential damages; (l) awarding Plaintiffs and the Class Members statutory damages and penalties, as allowed by law; (m) awarding Plaintiffs and Class Members restitution and disgorgement; (n) awarding Plaintiffs and the Class Members punitive damages against Facebook, GSR, Kogan, SCL Entities, and Cambridge, separately; (o) awarding Plaintiff and the Class Members pre-judgment and post-judgment interest; (p) awarding Plaintiff and the Class Members

reasonable attorneys' fees, costs, and expenses; and (q) granting such other relief as the Court deems just and proper.

Dated: April 10, 2018

CROSS & SIMON, LLC

/s/ Christopher P. Simon

Christopher P. Simon (No. 3697)
David G. Holmes (No. 4718)
1105 North Market Street, Suite 901
Telephone: (302) 777-4200
Facsimile: (302) 777-4224
csimon@crosslaw.com
dholmes@crosslaw.com

- and -

RUYAK CHERIAN LLP
Robert F. Ruyak (*pro hac vice* to be submitted)
Korula T. Cherian *(pro hac vice* to be submitted*)*
Richard Ripley (*pro hac vice* to be submitted)
Rebecca Anzidei (*pro hac vice* to be submitted)
1700 K Street NW, Suite 810
Washington, DC 20006
Telephone: (202) 838-1560
robertr@ruyakcherian.com
sunnyc@ruyakcherian.com
rickr@ruyakcherian.com
rebeccaa@ruyakcherian.com

- and -

FIELDS PLLC
Richard W. Fields (*pro hac vice* to be submitted)
1700 K Street, NW, Suite 810
Washington, DC 20006
(800) 878-1432
Fields@fieldslawpllc.com

- and -

MCCUE & PARTNERS, LLP
Matthew Jury (*pro hac vice* to be submitted)
Fourth Floor
158 Buckingham Palace Road
London SWIW 9TR
United Kingdom
matthew.jury@mccue-law.com

Counsel for Plaintiffs and Proposed Class